Configuring Avaya Breeze® platform with an Independent System Manager

Release 3.9
Issue 2
February 2024

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H 3 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 6
Purpose 6
Terminology 7
Supported versions 7
Prerequisites 7
Change history 8
Chapter 2: Overview 9
Avaya Aura® System Manager compatibility 9
Chapter 3: Configuration process 11
Configuration checklist 11
Chapter 4: Avaya Breeze® platform System Manager administration 14
Licensing the Avaya Aura® Media Server 14
Installing the Avaya Aura® Media Server license file 15
Installing the Avaya Breeze® platform license file 15
Creating a virtual Session Manager SIP entity 16
Administering an Avaya Breeze® platform SIP Entity 16
Administering an Avaya Breeze® platform instance 17
Creating a new cluster 18
Verifying the TLS version 21
Accepting new service 21
Verifying the management link 22
Chapter 5: Avaya Aura System Manager administration 23
Administering an Avaya Breeze® platform SIP entity 23
Enabling implicit users applications for SIP users 24
Chapter 6: Avaya Aura® Media Server administration 25
Adding the System Manager IP address 25
Administering Avaya Aura® Media Server for REST 26
Assigning Avaya Aura® Media Server for use with Avaya Breeze® platform 28
SIPS and SRTP on Avaya Aura® Media Server 28
Enabling and configuring digit relay settings 29
Chapter 7: Certificate management description 31
Installing the Avaya Aura® System Manager certificate on Avaya Breeze® platform 31
Installing the Avaya Breeze® platform System Manager certificate on Session Manager 32
Installing the System Manager certificate on Avaya Aura® Media Server 33
Verifying the Avaya Breeze® platform entity link connection 34
Verifying replication status 35
Chapter 8: Sample routing configuration 36
Creating an application and application sequence 36
Creating an implicit user rule 37

Creating a service profile 38
Assigning a service profile to implicit users 39
Chapter 9: Upgrading an independent System Manager configuration 41
Upgrade checklist 41
Chapter 10: Additional information 43
Documentation 43
Finding documents on the Avaya Support website 46
Avaya Documentation Center navigation 46
Training 47
Avaya Breeze® platform videos 48
Viewing Avaya Mentor videos 49
Developer resources 49
Support 50
Using the Avaya InSite Knowledge Base 50

Chapter 1: Introduction

Purpose

This document describes how to configure one or more Avaya Breeze® platform nodes in a SIP telephony network with a System Manager that is independent from the System Manager that controls Avaya Aura® components.

This configuration allows you to:

- Access Avaya Breeze® platform snap-ins without upgrading your Session Manager or Avaya Aura® Communication Manager. You can run different versions of System Manager for Avaya Aura® and Avaya Breeze® platform. You can also run different versions of System Manager for each independently managed Avaya Breeze® platform cluster.
- Manage different Avaya Breeze® platform clusters with different, independent System Manager instances. These may be independent of each other and independent of the System Manager that controls Avaya Aura® components. Currently, response times on a System Manager begin to slow down when the number of managed Avaya Breeze® platform nodes exceeds its documented limit. By installing more System Manager instances, you can increase the number of Avaya Breeze® platform nodes that can be managed.
- Isolate management of Avaya Breeze® platform clusters to different sets of administrators than those for Avaya Aura®. For example, you can route calls for subsets of users through an Avaya Breeze® platform cluster in a lab for trials without allowing access to the Avaya Aura® production system.

In this configuration, an “Avaya Aura® System Manager” manages Session Manager and Avaya Aura® Communication Manager.

The “Avaya Breeze® platform System Manager” manages Avaya Breeze® platform. You can have multiple Avaya Breeze® platform System Manager instances if you want to independently manage Avaya Breeze® platform clusters.

Avaya Aura® Media Server instances that are used by Avaya Breeze® platform are provisioned on the System Manager that manages a particular Avaya Breeze® platform node. Avaya Aura® Media Server instances that are used by Avaya Aura® Communication Manager are provisioned on the System Manager that manages Avaya Aura®. In this configuration, each System Manager that performs media processing must have a dedicated Avaya Aura® Media Server.

For SIP signalling:

- Each Avaya Breeze® platform System Manager must have a set of "virtual" Avaya Aura® Session Manager SIP entities

- Each Avaya Aura® System Manager that manages Avaya Aura® Session Manager must have a set of "virtual" Avaya Breeze® platform SIP entities

This document is intended for people who install and configure Avaya Breeze® platform at a customer site.

Related links

Terminology on page 7
Supported versions on page 7
Prerequisites on page 7
Change history on page 8

Terminology

Term	Definition
Avaya Aura® System Manager	System Manager Release 6.3 or higher that controls Avaya Aura® Release 6.3 or higher components, including Session Manager and Avaya Aura® Communication Manager.
Avaya Breeze® platform System Manager	System Manager that controls Avaya Breeze® platform and its snap-ins. See Avaya Aura System Manager compatibility on page 9.

Related links

Purpose on page 6

Supported versions

The following minimum versions have been tested for this configuration and are supported for it.

Component	Version
Avaya Aura® Communication Manager	6.3.18 (SP16)
Avaya Aura® Session Manager	6.3.18
Avaya Aura® System Manager	6.3.18
Avaya Aura® Media Server	8.0.2
Avaya Breeze® platform	3.8

Related links

Purpose on page 6

Prerequisites

Complete the following steps before beginning the procedures described in this document.

- For the Avaya Breeze® platform System Manager, deploy or upgrade to System Manager Release 8.0.1.2, 8.1.3 or 10.1. See Avaya Aura System Manager compatibility on page 9.

For more information about deploying System Manager, see *Deploying Avaya Aura® System Manager*.

- If running System Manager Release 8.0.1.2, you must install the Avaya Breeze® platform Element Manager using the `upgradeSolution` utility from the latest System Manager hot fix. See Deploying Avaya Breeze® platform.

- Deploy the Avaya Aura® Media Server OVA or upgrade to Avaya Aura® Media Server Release 8.0.x. For more information, see Deploying Avaya Breeze® platform.
  - For certificate management, your Avaya Aura® Media Server must be registered in DNS. If you do not use DNS, contact Avaya support for assistance.
- Deploy the Avaya Breeze® platform OVA or upgrade to Avaya Breeze® platform Release 3.9. For more information, see Deploying Avaya Breeze® platform.

  Important:
  - To configure Avaya Breeze® platform on the Avaya Breeze® platform System Manager, you must use the procedures in this document. Do not follow the procedures in Deploying Avaya Breeze® platform.
  - For certificate management, your Avaya Breeze® platform must be registered in DNS. If you do not use DNS, contact Avaya support for assistance.

Related links

Purpose on page 6

Change history

Issue	Date	Summary of changes
1	January 2024	• Update for Avaya Breeze® platform R3.9.
2	February 2024	• Corrections to web links to other Avaya Breeze® platform documents.

Chapter 2: Overview

To use Avaya Breeze® platform with an independent System Manager, you must:

- Add one or more System Manager R8.0.1.2, R8.1.3 or R10.1 instances into your environment as the Avaya Breeze® platform System Manager. See Avaya Aura System Manager compatibility on page 9.
  - If running System Manager Release 8.0.1.2, you must install the Avaya Breeze® platform Element Manager using the `upgradeSolution` utility from the latest System Manager hot fix. See Deploying Avaya Breeze® platform.
- Administer the Avaya Breeze® platform nodes on this System Manager.
- Configure the Avaya Aura® System Manager to place and route calls to the Avaya Breeze® platform nodes by way of Session Manager.

This gives calls from an Avaya Aura® system managed by a different System Manager access to Avaya Breeze® platform snap-ins.

Not supported

The following features and functions are not supported in this configuration:

- Engagement Call Control solution.
- userData DAO – Snap-ins will have no programmatic access to user data configured on the older System Manager.
- Authorization Service – The independent Avaya Breeze® platform System Manager has no comm profile/Communication Manager data. If there is a requirement for authenticating users, snap-ins can still get access tokens, but the tokens will not have any user-specific data apart from the user-id.

Related links

Avaya Aura System Manager compatibility on page 9

Avaya Aura® System Manager compatibility

The Avaya Breeze® platform can be deployed with System Manager R10.1.2.x, R10.1.3.x or R10.2.

System Manager	Notes
pre-R10.1.2	• If you are running System Manager Release 8.0.x, update to Release 10.1.2 or higher with the latest published hot fix from https://support.avaya.com.
R8.0.1.2	If running System Manager Release 8.0.1.2, you must install the Avaya Breeze® platform Element Manager using the `upgradeSolution` utility from the latest System Manager hot fix. See Deploying Avaya Breeze® platform. • When you have applied the latest Avaya Breeze® platform Element Manager to System Manager Release 8.0.1.2, subsequent integrated patches and hot fixes leave the Element Manager intact and no further action is required to work with Avaya Breeze® platform 3.9.x. If you are running System Manager Release 10.1.x, you must update your system to Release 8.1.3 with the latest published hot fix from https://support.avaya.com
R10.1.3.2/R10.2	These releases already contain the latest Avaya Breeze® platform Element Manager.

Related links

Overview on page 9

Chapter 3: Configuration process

Configuration checklist

Complete the tasks in this checklist to deploy Avaya Breeze® platform with an independent Avaya Aura® System Manager.

No.	Task	Reference/Notes	✔
1.	Verify that the Avaya Breeze® platform System Manager is deployed and administered with patches applied.	For the Avaya Breeze® platform System Manager, deploy or upgrade to System Manager Release 8.0.1.2, 8.1.3 or 10.1. See Avaya Aura System Manager compatibility on page 9. Deploy additional System Manager instances to independently manage different Avaya Breeze® platform clusters if desired.	
2.	Deploy the Avaya Breeze® platform OVA, providing the Avaya Breeze® platform System Manager IP address when needed.	Follow the OVA deployment procedures in Deploying Avaya Breeze® platform. **Important:** For Avaya Breeze® platform System Manager deployment administration, see the procedures in this document. Do not follow the procedures in Deploying Avaya Breeze® platform.	
3.	Deploy the Avaya Aura® Media Server OVA.	Follow the Avaya Aura® Media Server OVA deployment procedures in Deploying Avaya Breeze® platform.	
On each Avaya Breeze® platform System Manager complete the following tasks.			
4.	Install the Avaya Aura® Media Server license file.	See Licensing the Avaya Aura Media Server on page 14 and Installing the Avaya Aura Media Server license file on page 15	
5.	Install the Avaya Breeze® platform license file.	See Installing the Avaya Breeze platform license file on page 15	
6.	Create a virtual Session Manager SIP entity.	See Creating a virtual Session Manager SIP entity on page 16	

Table continues…

No.	Task	Reference/Notes	✔
7.	Create Avaya Breeze® platform SIP entities and entity links for each Avaya Breeze® platform node.	See Administering an Avaya Breeze platform SIP Entity on page 16	
8.	Administer an Avaya Breeze® platform instance for each node.	See Administering an Avaya Breeze platform instance on page 17	
9.	Create a new cluster, add Avaya Breeze® platform instances, and install snap-ins.	See Creating a new cluster on page 18	
10.	Verify TLS version support.	See Verifying the TLS version on page 21	
11.	Put the cluster in service.	See Accepting new service on page 21	
12.	Verify the management link for each Avaya Breeze® platform instance.	See Verifying the management link on page 22	
On the Avaya Aura® System Manager complete the following tasks. These steps are required only if you intend to route SIP calls to the separately managed Avaya Breeze® platform cluster.			
13.	Create a virtual Avaya Breeze® SIP entity and entity links for each Avaya Breeze® platform node to connect with Session Manager.	See Administering an Avaya Breeze platform SIP entity on page 23	
14.	Enable implicit user applications for SIP users.	See Enabling implicit users applications for SIP users on page 24	
Complete the following steps on the Avaya Aura® Media Server. These steps are required only if you intend to support media operations on SIP calls with the separately managed Avaya Breeze® platform cluster. If SIP calls or media operations are not supported, the Avaya Breeze® platform cluster does not require an associated Avaya Aura® Media Server.			
15.	Add the Avaya Breeze® platform System Manager IP address.	See Adding the System Manager IP address on page 25	
16.	Administer Avaya Aura® Media Server for REST.	See Administering Avaya Aura Media Server for REST on page 26 Avaya Aura® Media Server must be enrolled on System Manager. For more information, see System Manager enrollment information in *Implementing and Administering Avaya Aura® Media Server*.	
17.	Assign Avaya Aura® Media Server for use with Avaya Breeze® platform.	See Assigning Avaya Aura Media Server for use with Avaya Breeze platform on page 28 Complete this task on the new System Manager.	
18.	Administer SIPS and SRTP.	See SIPS and SRTP on Avaya Aura Media Server on page 28	
19.	Enable and configure digit relay settings.	See Enabling and configuring digit relay settings on page 29	

Table continues…

No.	Task	Reference/Notes	✔
Complete the following steps for certificate management among the components. These steps are required only if you intend to route SIP calls to the separately managed Avaya Breeze® platform cluster.			
20.	Install the Avaya Aura® System Manager Root CA certificate on each Avaya Breeze® platform node. If you are using a third-party CA, install that CA certificate instead of the System Manager CA.	See Installing the Avaya Aura System Manager certificate on Avaya Breeze platform on page 31	
21.	Install the Avaya Breeze® platform System Manager Root CA certificate on Session Manager. If you are using a third-party CA, install that CA certificate instead of the System Manager CA.	See Installing the Avaya Breeze platform System Manager certificate on Session Manager on page 32	
22.	Install the Avaya Aura® System Manager Root CA certificate on Avaya Aura® Media Server. If you are using a third-party CA, install that CA certificate instead of the System Manager CA.	See Installing the System Manager certificate on Avaya Aura Media Server on page 33	
23.	Verify the Entity Link Connection for each Avaya Breeze® platform instance.	See Verifying the Avaya Breeze platform entity link connection on page 34	
24.	Verify replication status for each Avaya Breeze® platform instance.	See Verifying replication status on page 35	
Complete the following steps to create a sample routing configuration. These steps are required only if you intend to route SIP calls to the separately managed Avaya Breeze® platform cluster.			
25.	On the Avaya Aura® System Manager, create a new application and application sequence.	See Creating an application and application sequence on page 36	
26.	On the Avaya Aura® System Manager, create a new Implicit User Pattern.	See Creating an implicit user rule on page 37	
27.	On the Avaya Breeze® platform System Manager, create a new Service Profile and add desired snap-ins to the profile.	See Creating a service profile on page 38	
28.	On the Avaya Breeze® platform System Manager, create a new Implicit User Profile and assign the Service Profile to it.	See Assigning a service profile to implicit users on page 39	
29.	In a system with multiple Avaya Breeze® platform nodes, administer SIP High Availability (HA) on the Avaya Aura® System Manager.	For more information, see HA administration content in Deploying Avaya Breeze® platform.	

Chapter 4: Avaya Breeze® platform System Manager administration

Related links

Licensing the Avaya Aura Media Server on page 14
Installing the Avaya Aura Media Server license file on page 15
Installing the Avaya Breeze platform license file on page 15
Creating a virtual Session Manager SIP entity on page 16
Administering an Avaya Breeze platform SIP Entity on page 16
Administering an Avaya Breeze platform instance on page 17
Creating a new cluster on page 18
Verifying the TLS version on page 21
Accepting new service on page 21
Verifying the management link on page 22

Licensing the Avaya Aura® Media Server

About this task

The license file installed on the System Manager WebLM and Avaya Aura® Media Server gets the license from System Manager WebLM.

Note:

- In accordance with the Avaya End User License Agreement (EULA) you can only administer the number of Avaya Aura® Media Server instances allowed by your Media Server license. For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Get the Avaya Aura® Media Server license from PLDS.
2. Install the Avaya Aura® Media Server license file on System Manager WebLM.
3. To configure Avaya Aura® Media Server with the System Manager WebLM IP address, perform the following steps:
    a. Navigate to **Licensing** > **General Settings**.

b. From the **Licensing** drop-down list, select **WebLM Server**.
c. Enter the address of the **WebLM Server** that you plan to use in the **Server Host Name or IP Address** field.
d. Enter the port to use with the **WebLM Server** in the **Server Port** field.
e. Enter the URL suffix used to identify the **WebLM Server**. The default URL suffix is `/WebLM/LicenseServer`.
f. In the **License Details** , set the **Maximum Number** and **Minimum Number** based on the number of sessions the cluster supports.
g. Click **Save**.

Related links

Avaya Breeze platform System Manager administration on page 14

Installing the Avaya Aura® Media Server license file

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install license** and **Browse** to the location of the Avaya Breeze® platform license file on your computer.
3. Click **Install**.

Related links

Avaya Breeze platform System Manager administration on page 14

Installing the Avaya Breeze® platform license file

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install license** and **Browse** to the location of the Avaya Breeze® platform license file on your computer.
3. Click **Install**.

Related links

Avaya Breeze platform System Manager administration on page 14

Creating a virtual Session Manager SIP entity

Before you begin

Get the IP address of the Session Manager Security Module interface and the SIP Entity name.

About this task

Complete this task to administer Session Manager as a SIP entity on the Avaya Breeze® platform System Manager to act as a pointer to the Session Manager SIP entity on the Avaya Aura® System Manager.

Procedure

1. On System Manager, click **Elements** > **Routing** > **SIP Entities** and click **New**.
2. In the **Name** field, type the name of your SIP entity.
3. In the **FQDN or IP Address** field, type the IP address of your Session Manager Security Module.
4. In the **Type** field, click **Session Manager**.
5. Click **Commit** to save your changes.
6. Repeat this procedure for each Session Manager administered on the Avaya Aura® System Manager.

Related links

Avaya Breeze platform System Manager administration on page 14

Administering an Avaya Breeze® platform SIP Entity

Before you begin

Get the IP address of the Avaya Breeze® platform Security Module interface and the SIP Entity name.

About this task

Administer Avaya Breeze® platform as a SIP Entity so that you can configure Session Manager to route traffic through Avaya Breeze® platform. Create an Entity Link to connect Session Manager to Avaya Breeze® platform. You must administer separate Entity Links for Avaya Breeze® platform nodes to open SIP listeners on the designated ports.

Note:

This procedure assumes you are using the TLS protocol. TLS is the recommended protocol for production environments since it is secure and encrypted. Should the need arise to take a network trace between Session Manager and Avaya Breeze® platform, change the protocol to TCP. If this is a production environment, change the protocol back to TLS as soon as the trace is complete.

Procedure

1. On System Manager, click **Elements** > **Routing** > **SIP Entities** and click **New**.
2. In the **Name** field, type the name of your SIP Entity.

   The SIP Entity name is automatically used as your Avaya Breeze® platform instance name when you create the Avaya Breeze® platform instance.
3. In the **FQDN or IP Address** field, type the IP address of your Avaya Breeze® platform Security Module.
4. From the **Type** drop-down menu, select `Avaya Breeze`.
5. From the **Loop Detection Mode** drop-down menu, select `Off`.
6. From the **SIP Link Monitoring** drop-down menu, select `Link Monitoring Enabled`.
7. Under Entity Links, click Add.
8. For SIP Entity 1, select the virtual Session Manager SIP Entity you created.
9. Click **Commit** to save your changes.

Related links

Avaya Breeze platform System Manager administration on page 14

Administering an Avaya Breeze® platform instance

About this task

You can create and administer the number of Avaya Breeze® platform instances allowed by the Avaya Breeze® platform license.

You set the FQDN of the Avaya Breeze® platform **Management Network Interface** to the same IP address you used when deploying the virtual machine.

System Manager supports HTTP Cookie based Single Sign On (SSO). To facilitate SSO between System Manager and Avaya Breeze® platform, the domain name component of Avaya Breeze® platform FQDN must match all or at least a part of the domain name of System Manager FQDN.

Before you begin

Ensure that you have the following:

- The IPv4 address or the FQDN of the Avaya Breeze® platform **Management Network Interface**.
- (Optional) The IPv6 address or the FQDN of the Avaya Breeze® platform **Management Network Interface**. You must enter the IPv4 address even if administering an IPv6 address.

  Important:

  During OVA deployments do not enter the IPv6 address, IPv6 network prefix, or IPv6 gateway for eth0 unless the latest Avaya Breeze® platform patches already have

been applied. For more information about configuring IPv6, see “Enabling IPv6 on the management interface of an Avaya Breeze platform server” in Deploying Avaya Breeze® platform.

- An Avaya Breeze® platform management FQDN that is registered in DNS.
- The IPv4 or IPv6 address including the IPv4 network mask or IPv6 Network prefix length, and IPv4 or IPv6 default gateway for the Avaya Breeze® platform **Security Module**.
- The SIP entity name associated to the Avaya Breeze® platform **Security Module**.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
2. In the Avaya Breeze® Server Instances list, click **New**.
3. In the **SIP Entity** field, click the SIP Entity that you created.
4. Ensure that the value in the **UCID Network Node ID** field is unique across the solution deployment so that it does not conflict with other UCID-generating entities such as Avaya Aura® Communication Manager or Avaya Experience Portal.

   UCID Network Node ID is a unique, numeric node ID that is assigned to each Avaya Breeze® platform server provisioned.

   The UCID Network Node ID must be unique across both System Manager instances.
5. In the Management Network Interface **FQDN or IPv4 Address** field, type the IP address or FQDN of the Avaya Breeze® platform **Management Network Interface**.
6. **(Optional)** In the Management Network Interface **FQDN or IPv6 Address** field, type the IPv6 address or FQDN of the Avaya Breeze® platform **Management Network Interface**.
7. In the Security Module fields, type the required addresses for the IPv4 or IPv6 SIP Entity Address, Network Mask or Network prefix length, and Default Gateway used for the SIP (Security Module) network.
8. Click **Commit** to save your changes.

   The Commit fails if the Avaya Breeze® platform license file on WebLM does not have the sufficient capacity to allow addition of another Avaya Breeze® platform server.

Related links

Avaya Breeze platform System Manager administration on page 14

Creating a new cluster

Before you begin

Load the required services or bundles for your cluster on the Service Management page on the New System Manager.

About this task

Use the Cluster Editor page to:

- Select a cluster profile.
- Configure the cluster attributes.
- Add Avaya Breeze® platform servers to a cluster.
- Install snap-ins on a cluster.

You must set up user name and password for Avaya Aura® Media Server if basic authentication is used in Avaya Aura® Media Server administration.

See Administering Avaya Breeze® platform for information about additional available features.

Warning:

Avaya Breeze® platform supports VMware HA, but different applications running on Avaya Breeze® platform may not. Refer to the application deployment guide before deploying Avaya Breeze® platform into an HA-enabled data center. For applications that do not support VMware HA, Avaya Breeze® platform itself can provide an HA solution if each node in a cluster is deployed on a different VMware host.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the cluster profile of your choice.

   Note:

   You must select a cluster profile to view the appropriate cluster attributes.

   For example, select the general purpose cluster profile or a product specific cluster profile.

   Refer to the snap-in reference documentation for the cluster profile appropriate for the use case being deployed.
4. Enter the cluster attributes for your cluster. You can edit the default cluster attributes the system displays.

   The name and the IP address of a cluster must be unique.

   You cannot edit all the cluster attributes. Some attributes are read-only.

   Note:

   Do not assign a **Cluster IP** for a single-node cluster.
5. If you will be installing snap-ins that use the cluster database, select the **Enable Cluster Database** check box.

   Note:

   If you attempt to install a snap-in using the cluster database on a cluster that has the **Enable Cluster Database** feature disabled, the installation will be blocked.

6. In the **Minimum TLS Version for SIP Call Traffic** field, specify the TLS version which will be used for SIP calls intercepting Avaya Breeze® platform.
7. In the **Minimum TLS Version for Non-SIP Call Traffic** field, specify the TLS version which will be applied for HTTP requests to Avaya Breeze® platform.
8. (Optional) Click the **Servers** tab to assign Avaya Breeze® platform servers to the cluster.

   Important:

   Do not assign servers with different releases to the same cluster. All servers in the cluster should be running the same Avaya Breeze® platform version.

   For more information on upgrading clusters, see Upgrading Avaya Breeze® platform.
9. **(Optional)** Click the **Services** tab to assign snap-ins to this cluster.

   When you assign snap-ins to a cluster, the highest version of the required snap-ins are automatically assigned to the cluster for installation. For the product specific cluster profiles, you must load the required snap-ins from the Service Management page before you install the snap-in.

   In the **Select TLS Version for Selected Snap-in** field, select the TLS version of the snap-in:

   - **Default**

     If you select **Default**, the Avaya Breeze® platform uses the **Minimum TLS Version** field value set in the System Manager global configuration.
   - **TLS v1.0**
   - **TLS v1.2**
   - **TLS v1.3**

     Avaya recommends using TLS v1.3.
10. Click **Commit** to create the cluster.

    The **Service Install Status** in the Cluster Administration page displays a green tick symbol after all the assigned snap-ins are successfully installed on all the servers in the cluster.

    To view the Avaya Breeze® platform servers in the cluster, click **Show** in the **Details** column of the cluster. The system displays the members of the cluster, and the status of each instance in the cluster.

    Click a specific Avaya Breeze® platform server to go to the Avaya Breeze® Instance Editor page. You can view and edit the properties of the Avaya Breeze® platform server from this page.

    Note:

    When you administer a new Avaya Breeze® platform server, you must add the server to a cluster. If you do not add the Avaya Breeze® platform server to a cluster, you cannot install snap-ins on that server.

Related links

Avaya Breeze platform System Manager administration on page 14

Verifying the TLS version

About this task

Your Avaya Aura® System Manager may support TLS v1.0, v1.2 or v1.3. Check your Avaya Aura® System Manager documentation to determine which TLS version your System Manager supports. Use this procedure to verify that your Avaya Breeze® platform System Manager is administered for the correct TLS version.

Procedure

1. On the Avaya Breeze® platform System Manager under **Services**, select **Security** > **Configuration** > **Security Configuration**.
2. For the **Minimum TLS Version**, select the TLS version supported by your Avaya Aura® System Manager.
3. Click **Commit** to save your changes.

Related links

Avaya Breeze platform System Manager administration on page 14

Accepting new service

About this task

The steps for returning the server to service are different depending on if the server is being added to an existing in-service cluster or if it is being added as part of a new cluster. Follow the steps appropriate to your situation.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select a cluster and assign your Avaya Breeze® platform server to the cluster.
3. If this is a new cluster, put the cluster in service.
    a. From the **Cluster State** drop-down menu, select **Accept New Service**.
    b. Verify that the **Cluster State** column for the cluster changed to **Accepting**.
4. If you are adding the server to an existing cluster that is in service, accept service for the server.
    a. On System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.

b. Click the checkbox in front of the new server.
c. From the **System State** drop-down menu, select **Accept New Service**.
d. Verify that the **System State** column for the server changed to **Accepting**.

Related links

Avaya Breeze platform System Manager administration on page 14

Verifying the management link

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**.
2. Check the **Tests Pass** column.
   - A green check mark indicates that the management link is up and healthy.
   - Dashes indicate that the management link is still initializing and is not up yet.
   - A red cross indicates that the management link is down.

   For more information, see Maintaining and Troubleshooting Avaya Breeze® platform.

Related links

Avaya Breeze platform System Manager administration on page 14

Chapter 5: Avaya Aura System Manager administration

Related links

Administering an Avaya Breeze platform SIP entity on page 23
Enabling implicit users applications for SIP users on page 24

Administering an Avaya Breeze® platform SIP entity

Before you begin

Get the IP address of the Avaya Breeze® platform Security Module interface and the SIP entity name.

About this task

Administer a virtual Avaya Breeze® platform SIP entity and entity links for Session Manager to point to Avaya Breeze® platform nodes. Create an entity and links for each Avaya Breeze® platform node.

You must complete this procedure even if you do not intend to route SIP calls to the separately managed Avaya Breeze® platform cluster. The term SIP entity identifies the Avaya Breeze® platform traffic interface. On Avaya Breeze® platform, that traffic can be SIP, HTTP, or any other TCP/IP protocol, exclusively or mixed. On System Manager all are referred to as a SIP entity.

Procedure

1. On the Avaya Aura® System Manager, click **Elements** > **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, type the name of your SIP entity.
4. In the **FQDN or IP Address** field, type the IP address of your Avaya Breeze® platform Security Module.
5. In the **Type** field, click `Avaya Breeze`.

   If your Avaya Aura® System Manager is a release prior to 7.0, click `Collaboration Environment`.
6. In **Entity Links**, click **Add**.

7. For SIP Entity 1, click the virtual Session Manager SIP entity that you created.
8. For SIP Entity 2, click the Avaya Breeze® platform SIP entity that you just created.
9. Click **Commit** to save your changes.

Related links

Avaya Aura System Manager administration on page 23

Enabling implicit users applications for SIP users

About this task

This procedure is required for calling-party and called-party snap-ins.

Note:

You must perform this procedure only once.

Procedure

1. On System Manager, click **Elements** > **Session Manager** > **Global Settings**.
2. Select **Enable Implicit Users Applications for SIP users**.
3. Click **Commit**.

Related links

Avaya Aura System Manager administration on page 23

Chapter 6: Avaya Aura® Media Server administration

Related links

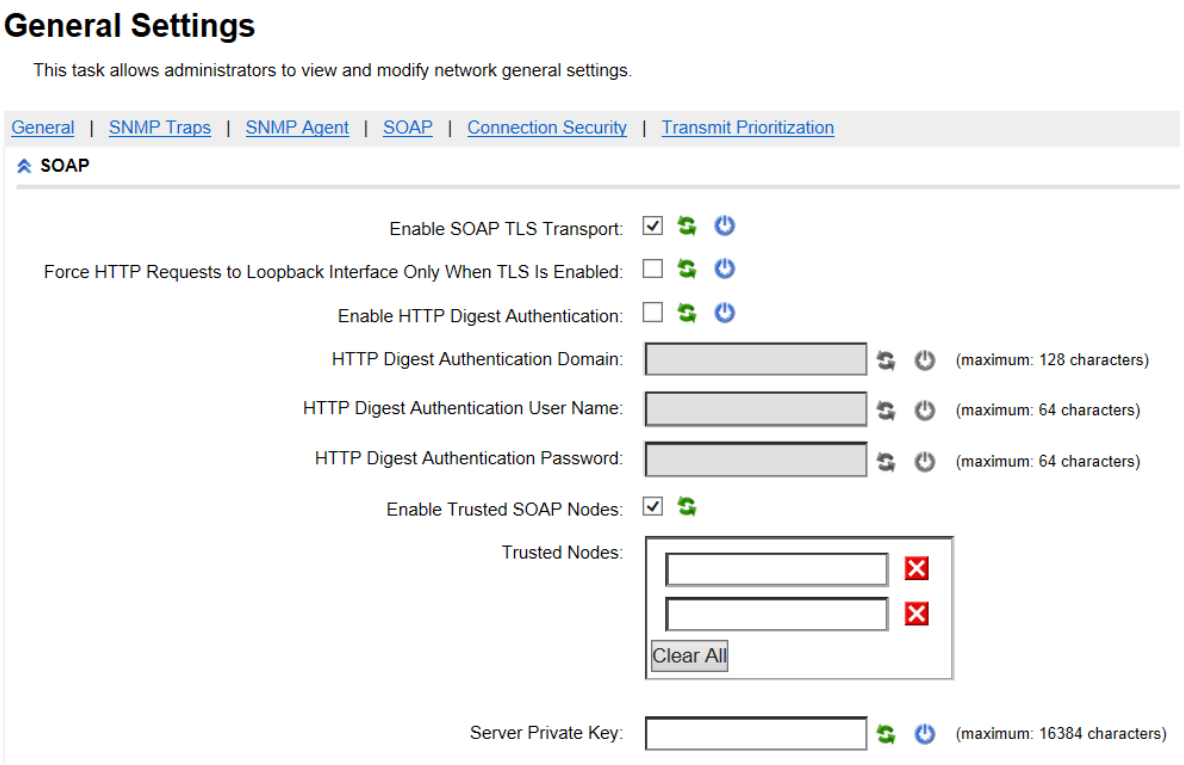
Adding the System Manager IP address on page 25
Administering Avaya Aura Media Server for REST on page 26
Assigning Avaya Aura Media Server for use with Avaya Breeze platform on page 28
SIPS and SRTP on Avaya Aura Media Server on page 28
Enabling and configuring digit relay settings on page 29

Adding the System Manager IP address

Procedure

1. Type `https://<fqdn>:8443/emlogin` in a Web browser.
2. Log on to the Avaya Aura® Media Server Element Manager interface using the customer login ID and password created when you deployed the OVA.

3. Navigate to **System Configuration** > **Network Settings** > **General Settings**.



4. In the **SOAP** section, **Trusted Nodes** field, type the IP address of the primary System Manager that is used to manage Avaya Breeze® platform. If this is a geo-redundant deployment, type the secondary System Manager IP addresses in the second text field in the Trusted Nodes box.
5. Click **Save** .
6. Repeat this procedure for each Avaya Aura® Media Server.

Next steps

Configure announcements for services on each Avaya Aura® Media Server. For additional information, see *Media File Provisioning* in *Implementing and Administering Avaya Aura® Media Server*. All Media Servers must be configured with the same announcement files.

Related links

Avaya Aura Media Server administration on page 25

Administering Avaya Aura® Media Server for REST

About this task

Use this procedure to configure Avaya Aura® Media Server to allow REST access using HTTP.

For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Before you begin

Avaya Aura® Media Server must be enrolled on System Manager. For additional information, see the System Manager enrollment section in *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Log on to the Avaya Aura® Media Server web console.
2. Navigate to **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.
3. To enable TLS for REST services, select the **Enable TLS Transport** check box.
4. To enable two-way authentication for an extra level of security, select the **Enable TLS Mutual Authentication** check box.
5. To use plaintext usernames and passwords, select **Basic Authentication**. Alternatively, to include an authentication realm and encrypt the credentials before sending them over the network, select **Digest Authentication**.
    a. Enter the required username and password credentials in the **Authentication Username** and **Authentication Password** fields.
    b. If you selected **Digest Authentication**, then enter the name of the required authentication realm in the **Authentication Realm** field.
6. Click **Save**.

    Changes to the transport settings require a restart to take effect.
7. Navigate to **System Configuration** > **Network Settings** > **General Settings** > **Connection Security**.
8. Select the **Verify Host Name of TLS Client Connections** check box.
9. Click **Save**.
10. Navigate to **Security** > **Certificate Management** > **Key Store**.
11. Assign System Manager signed certificate to all service profiles.
12. Click **Save**.
13. Restart Avaya Aura® Media Server:
    a. Navigate to **System Status** > **Element Status**.
    b. Click **Restart**.

Related links

Avaya Aura Media Server administration on page 25

Assigning Avaya Aura® Media Server for use with Avaya Breeze® platform

Procedure

1. In System Manager, click **Elements** > **Media Server** > **Application Assignment**.
2. Select the check box next to Avaya Breeze® platform, and click **Edit**.
3. Select the check box next to Avaya Aura® Media Server and click **Commit**.

   The system can take up to two minutes to update Avaya Breeze® platform.

   You cannot assign Avaya Aura® Media Server to multiple applications.

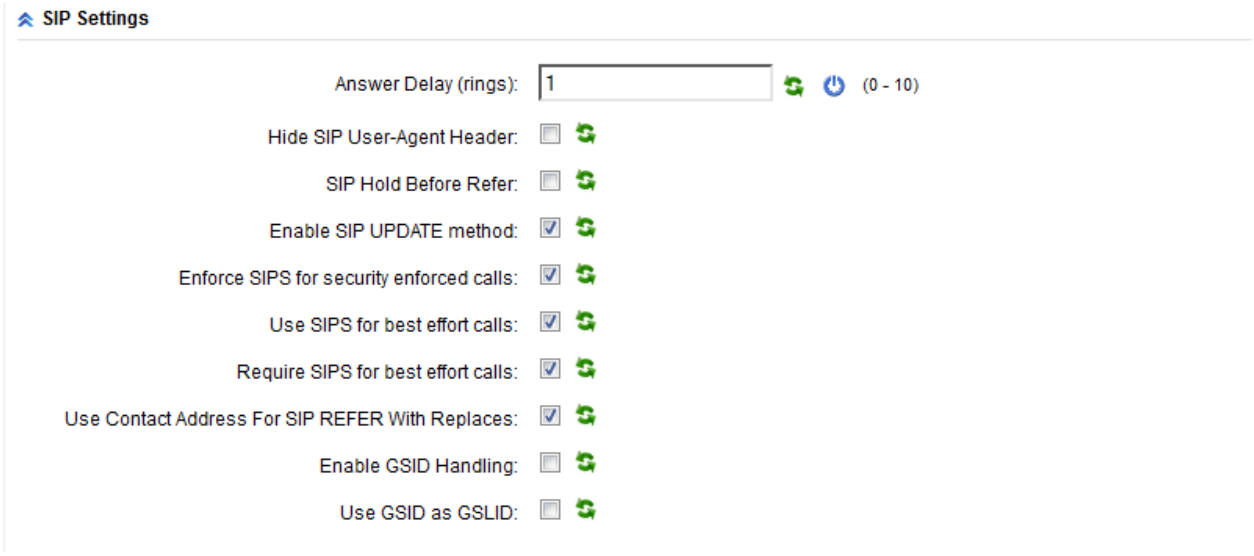
Related links

Avaya Aura Media Server administration on page 25

SIPS and SRTP on Avaya Aura® Media Server

The Secure Real Time Protocol (SRTP) administration is described in detail in the *Implementation and Administering Avaya Aura Media Server* document, specifically the topics on Configuring SIP general settings and Media security configuration. Refer to the Avaya Aura® Media Server Element Manager example below for interoperability with Avaya Aura.

The SIPS settings are found under **Home** > **System Configuration** > **Signaling Protocols** > **SIP** > **General Settings**.



The SRTP settings are found under **Home** > **System Configuration** > **Media Processing** > **Media Security**.

If you set the **Security Policy** field to **BEST EFFORT**, you must select the following fields in the SIP Settings section:

- **Enforce SIPS for security enforced calls**
- **Require SIPS for best effort calls**

Related links

Avaya Aura Media Server administration on page 25

Enabling and configuring digit relay settings

About this task

Note:

Controlling applications typically override AAMS configuration using templates and template control modifiers. Digit relay configuration changes and preferences must be configured first on the controlling application and not on Avaya Aura® MS. See documentation for the controlling application to determine if any Avaya Aura® MS changes are required.

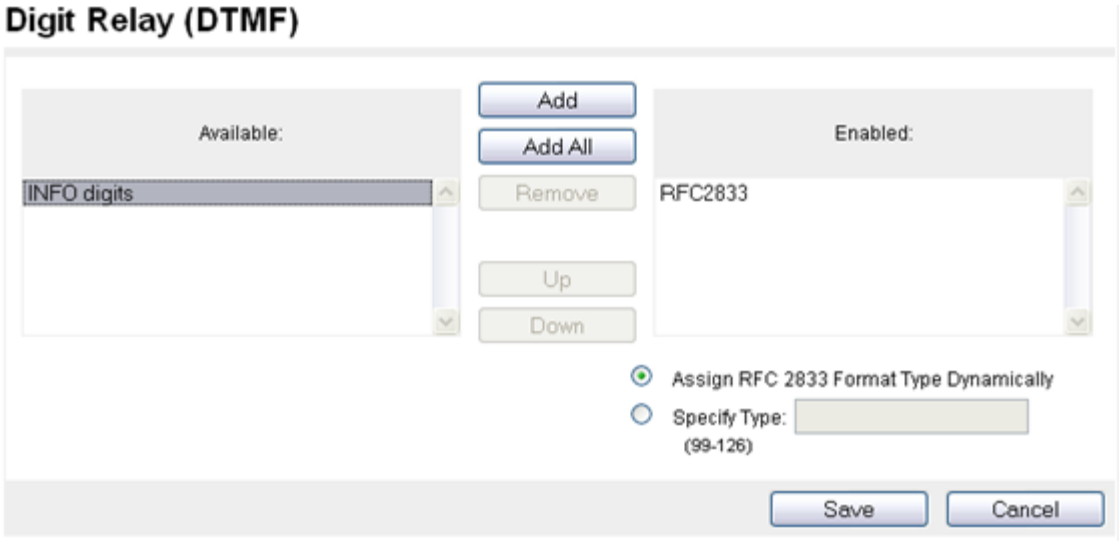
Avaya Aura® MS uses digit relay settings and the order of the enabled relay methods when negotiating digit relay with a client endpoint. These settings apply for inbound or outbound sessions.

Avaya Aura® MS also supports in-band DTMF. The system defaults to this option if no other option is configured or negotiated by Avaya Aura® MS. The preferred method of digit transmission is RFC 2833.

Perform the following procedure to enable and configure the digit relay support on Avaya Aura® MS.

Procedure

1. Navigate to **EM** > **System Configuration** > **Media Processing** > **Digit Relay (DTMF)**.



2. On the Digit Relay (DTMF) page, select one or more methods from the **Available** list.
3. Click **Add** to move the methods to the **Enabled** list.
4. To change the priority rank of a method within the **Enabled** list, select a method and use the **Up** or **Down** buttons to move it within the list.
5. Choose the required payload type option:
   - If a dynamic payload type is required, select **Assign RFC 2833 Format Type Dynamically**.
   - If a fixed payload type is required, select **Specify Type**. In the **Specify Type** field, enter the value to use in the payload type field of the RTP header when transmitting RFC2833 encoded digits.
6. Click **Save**.

Related links

Avaya Aura Media Server administration on page 25

Chapter 7: Certificate management description

The elements managed by the Avaya Breeze® platform System Manager will have default certificates issued by the Avaya Breeze® platform System Manager CA. The elements managed by the Avaya Aura® System Manager will have certificates issued by the Avaya Aura® System Manager CA. For the various elements to trust each other, the CA from each System Manager must be added as a trusted CA certificate for elements managed by the other. To establish this trust, follow the procedures in this chapter . If you are using a third-party CA, install the certificate from that CA across all systems.

Related links

Installing the Avaya Aura System Manager certificate on Avaya Breeze platform on page 31
Installing the Avaya Breeze platform System Manager certificate on Session Manager on page 32
Installing the System Manager certificate on Avaya Aura Media Server on page 33
Verifying the Avaya Breeze platform entity link connection on page 34
Verifying replication status on page 35

Installing the Avaya Aura® System Manager certificate on Avaya Breeze® platform

About this task

Use this procedure to install the certificate only for the TLS protocol. First you must download the Root CA certificate from the Avaya Aura® System Manager. Then you must install the Root CA certificate on each Avaya Breeze® platform node.

Procedure

1. On the Avaya Aura® System Manager, click **Services** > **Security** > **Certificates** > **Authority**.
2. Do one of the following:
   - If your Avaya Aura® System Manager is release 7.1 or later, click **CA Structure & CRLs** and then click **Download pem file.**

- If your Avaya Aura® System Manager is an earlier release, click **Download pem file.**

3. On the Avaya Breeze® platform System Manager, click **Services** > **Inventory** > **Manage Elements**.
4. Select the check box in front of the Avaya Breeze® platform node.
5. In the **More Actions** menu, click **Manage Trusted Certificates**.
6. On the Trusted Certificates page, click **Add**.
7. Click **Import from file**, and navigate to the location where you saved the Root CA certificate.
8. Click **Open**.
9. When System Manager displays the certificate next to **Please select a file**, click **Retrieve Certificate**.

   The Certificate Details display.
10. Click **Commit**.

    The imported certificate displays in the Trusted Certificates list.
11. Click **Done**.
12. Download the certificate to each Avaya Breeze® platform node.

Related links

Certificate management description on page 31

Installing the Avaya Breeze® platform System Manager certificate on Session Manager

About this task

Use this procedure to install the certificate only for the TLS protocol. First you must download the Root CA certificate on the Avaya Breeze® platform System Manager. Then you must install the Root CA certificate on Session Manager.

Procedure

1. On the Avaya Breeze® platform System Manager, in **Services**, click **Security** > **Certificates** > **Authority** > **CA Structures & CRLs** .
2. Click **Download pem file.**
3. On the Avaya Aura® System Manager, click **Services** > **Inventory** > **Manage Elements**.
4. Check the box in front of the Session Manager element.

5. Under the **More Actions** menu, do one of the following:
   - If your Avaya Aura® System Manager is release 7.1 or later, click **Manage Trusted Certificates**.
   - If your Avaya Aura® System Manager is an earlier release, click **Configure Trusted Certificates**.
6. On the Trusted Certificates page, click **Add**.
7. Click **Import from file**, and navigate to the location where you saved the Avaya Breeze® platform System Manager Root CA certificate.
8. Click **Open**.
9. When System Manager displays the certificate next to **Please select a file**, click **Retrieve Certificate**.

   The Certificate Details display.
10. Click **Commit**.

    The imported certificate displays in the Trusted Certificates list.
11. Click **Done**.

Related links

Certificate management description on page 31

Installing the System Manager certificate on Avaya Aura® Media Server

Before you begin

For this procedure use the System Manager certificate for the System Manager that manages the Avaya Breeze® platform node.

Procedure

1. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
2. Click **Import ...** on the Trust Store page.
3. Click **Browse...** and select the System Manager certificate.
4. Click **Upload**.
5. Verify the certificate information.
6. Enter a name in the **Trust friendly name** field for each certificate.
7. Click **Save**.
8. To restart the media server and apply the changes, click **Confirm**.

   To restart later, click **Cancel**.

Related links

Certificate management description on page 31

Verifying the Avaya Breeze® platform entity link connection

About this task

Complete this task to verify that Session Manager can connect with Avaya Breeze® platform using the SIP entity link. To do this you must first verify the status of SIP link monitoring on the Session Manager instance.

The task verifies the link between Avaya Breeze® platform nodes and the virtual Session Manager entity you created.

Procedure

1. Modify the Session Manager Instance.
   a. On System Manager, click **Elements** > **Session Manager** > **Session Manager Administration**.
   b. Select the Session Manager instance that you linked to Avaya Breeze® platform. Click **Edit**.
   c. Check **Enable Monitoring** in the **Monitoring** section.
   d. Click **Commit**.
2. Test the entity link.
   a. On System Manager, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.
   b. Click the name of the Session Manager instance that you linked to Avaya Breeze® platform.

      The system displays a list with the status of all the entity links for the selected Session Manager.
   c. Locate the Avaya Breeze® platform SIP entity and check the **Conn. Status** column.
      - If you see `UP`, the link to Session Manager is successful.
      - If you do not see `UP`, for additional information, see *Avaya Breeze® platform FAQ and Troubleshooting for Service Developers*.

Related links

Certificate management description on page 31

Verifying replication status

About this task

Complete this task to verify that the System Manager database has replicated to Avaya Breeze® platform.

This task verifies that the Avaya Breeze® platform nodes are registering and replicating correctly with the Avaya Breeze® platform System Manager.

Procedure

1. In System Manager, click **Services** > **Replication**.
2. Locate the Avaya Breeze® platform in the **Replica Group** list.
3. In the **Synchronization Status** column, verify that the Avaya Breeze® platform status is `Synchronized`.
   - Depending on the amount of data, the replication might take some time to complete. Refresh the page or periodically recheck the status.
   - If the status is not `Synchronized`, for more information, see Maintaining and Troubleshooting Avaya Breeze® platform.

Related links

Certificate management description on page 31

Chapter 8: Sample routing configuration

The following tasks configure a specific pattern that Avaya Aura® System Manager will use to determine when to route SIP calls to Avaya Breeze® platform.

1. On the Avaya Aura® System Manager:
   a. Create an Application and Application Sequence used by Session Manager to route calls to Avaya Breeze® platform as represented by the virtual Avaya Breeze (or Collaboration Environment) SIP Entity.
   b. Create an Implicit User Rule which determines which calls are routed to Avaya Breeze® platform.
2. On the Avaya Breeze® platform System Manager:
   a. Create a Service Profile, which determines what snap-ins are accessed when a call routes to Avaya Breeze® platform.
   b. Create an Implicit User Profile and assign it a Service Profile to determine which calls route to a Service Profile and access its associated snap-ins.

Related links

Creating an application and application sequence on page 36
Creating an implicit user rule on page 37
Creating a service profile on page 38
Assigning a service profile to implicit users on page 39

Creating an application and application sequence

About this task

Create the application and application sequence on the Avaya Aura® System Manager. If you are using an Avaya Aura® System Manager release that is earlier than 7.1, steps for creating an application and application sequence might be slightly different. For more information, see the Avaya Breeze® platform documentation for your release.

Use this procedure to administer the Avaya Breeze® platform SIP entity or Avaya Breeze® platform HA cluster SIP entity as an application and then make that application part of an application sequence.

You create the application and application sequence only once per Avaya Breeze® platform SIP entity or Avaya Breeze® platform HA cluster SIP entity cluster. The application sequence is used

for routing calls to Avaya Breeze® platform by Session Manager using the implicit user pattern scope. If you already have an application and application sequence for Avaya Breeze® platform, you can skip this procedure.

Procedure

1. On System Manager, click **Elements** > **Session Manager** > **Application Configuration** > **Applications**.
2. Click **New**.
3. Type the name for your application.

   For example, `Avaya Breeze`.
4. For the **SIP Entity**, select the Avaya Breeze® platform server where your snap-in resides.

   Select the virtual Avaya Breeze (or Collaboration Environment) SIP entity representing the Avaya Breeze® platform instance.

   The SIP entity might represent a SIP load balancing FQDN.

   For information about creating the SIP entity, see Deploying Avaya Breeze® platform
5. To save your changes, click **Commit**.
6. On the **Session Manager** menu under **Application Configuration**, click **Application Sequences** and click **New**.
7. Type the name of your new application sequence.

   For example, type `Avaya Breeze Application Sequence`.
8. In the list of **Available Applications** click **+** by the Avaya Breeze® platform application that you created.
9. If you do not want calls to fail when Avaya Breeze® platform is unavailable, uncheck the **Mandatory** check box. Session Manager stops processing a call if it cannot reach a mandatory application.
10. To save your application sequence, click **Commit**.

Related links

Sample routing configuration on page 36

Creating an implicit user rule

About this task

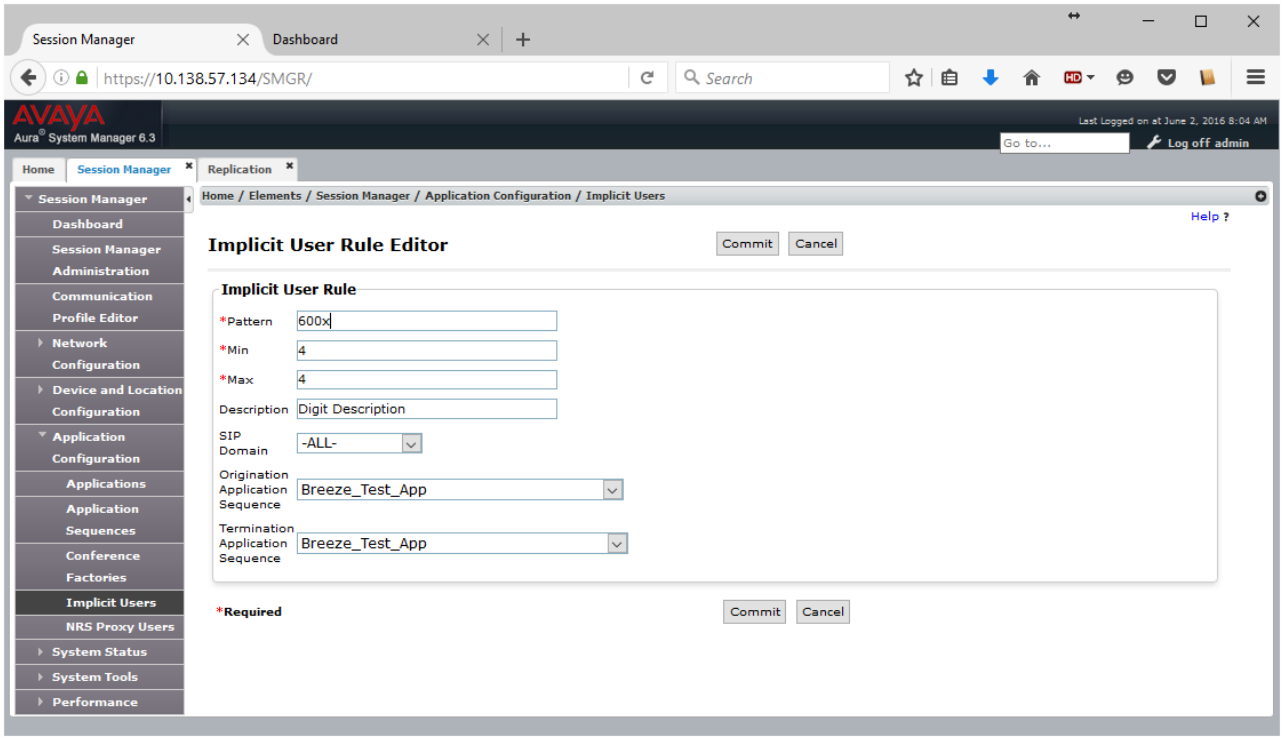
Create the implicit user rule on the Avaya Aura® System Manager. The implicit user rule creates a numeric pattern that the Avaya Aura® System Manager monitors. When a call matches the pattern, the Avaya Aura® System Manager routes the call to Avaya Breeze® platform.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Application Configuration** > **Implicit Users**.
2. Click **New**.
3. On the Implicit User Rule Editor page, enter the appropriate information.
4. Click **Commit**.

Example

For example in the rule below, the Avaya Aura® System Manager will look for a four-digit pattern starting with 600x (6000-6009) in all configured SIP domains. Configure your Avaya Breeze® platform Test App for both originating and terminating application sequences. Any call originating from a station matching 600x or anyone calling a station matching 600x will route to the Avaya Breeze® platform node identified in the application sequence.



Related links

Sample routing configuration on page 36

Creating a service profile

About this task

Create the service profile on the Avaya Breeze® platform System Manager.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®**.
2. In the navigation pane, click **Configuration** > **Service Profiles**.
3. Click **New**.
4. In the **Identity** section, enter a descriptive name for the service profile.
5. Optionally type a **Description** of the service profile.
6. In the **Available Service to Add to this Service Profile** list, complete one of the following steps.
   - To add the latest version of the service, click the **+** sign next to the **Name** of the service you want to add to the service profilee.
   - To add an alternate version of the service, click **Advanced** next to the **Name** of the service you want to add to the service profile. From the **Service Version** drop-down menu, select the version you want.
7. Click **Commit** to save this service profile.

Related links

Sample routing configuration on page 36

Assigning a service profile to implicit users

Before you begin

You must create the service profile before it can be assigned.

About this task

Create the implicit user profile on the Avaya Breeze® platform System Manager. The implicit user profile rule determines which service profile System Manager applies to the matched pattern.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®**.
2. In the left navigation pane, click **Configuration** > **Implicit User Profiles.**
3. Click **New** to create a new rule, or select a pattern and click **Edit** to change an existing rule.
4. In the **Service Profile** field select the service profile for these users.
5. In the **Pattern** field specify the pattern as defined for the called or calling party number.
6. **(Optional)** Revise the **Min** and **Max** values for the number of digits from the pattern to match.

   These fields auto-populate based on the pattern.

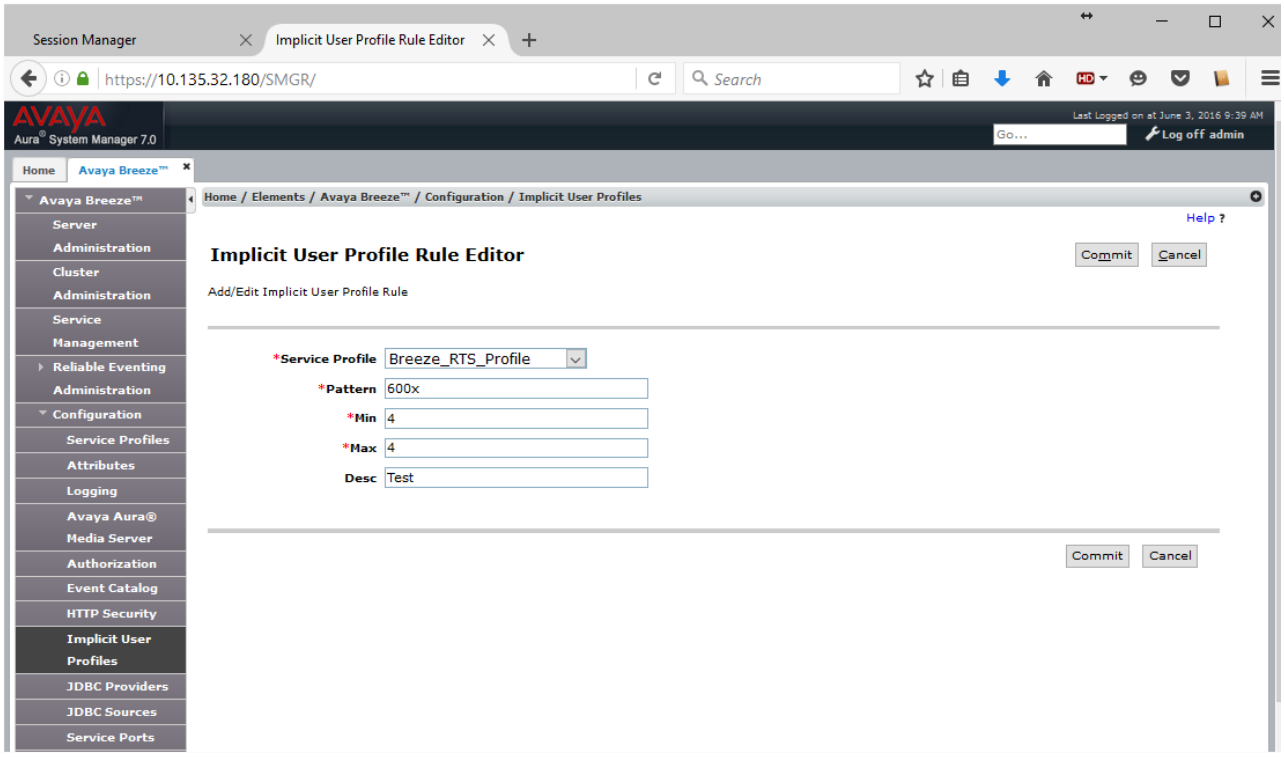
7. Type a description for the rule.

   You can provide a description of the group of users the rule defines.

8. Click **Commit** to save your changes.

Example

In this routing example, create an implicit user profile that matches the implicit user rule that you created on the Avaya Aura® System Manager.



Related links

Sample routing configuration on page 36

Chapter 9: Upgrading an independent System Manager configuration

Upgrade checklist

Complete the tasks in this checklist to upgrade Avaya Breeze® platform in a configuration with an independent System Manager.

No.	Task	Reference/Notes	✔
1.	Verify that the Avaya Breeze® platform System Manager is upgraded and administered with patches applied.	If running System Manager Release 8.0.1.2, you must install the Avaya Breeze® platform Element Manager using the `upgradeSolution` utility from the latest System Manager hot fix. See Deploying Avaya Breeze® platform.	
2.	Upgrade the Avaya Aura® Media Server.	For information about upgrading Avaya Aura® Media Server, see *Implementing and Administering Avaya Aura® Media Server*, and Upgrading Avaya Breeze® platform. Due to certificate management, your Avaya Aura® Media Server must be registered in DNS. If you do not use DNS, contact Avaya support for assistance.	
3.	Upgrade Avaya Breeze® platform providing the Avaya Breeze® platform System Manager IP address if needed.	Follow upgrade procedures in Upgrading Avaya Breeze® platform.	
4.	On the Avaya Breeze® platform System Manager verify the TLS version support.	Verifying the TLS version on page 21	
5.	Install a new Avaya Aura® Media Server license file.	Licensing the Avaya Aura Media Server on page 14, Installing the Avaya Aura Media Server license file on page 15	

Table continues…

No.	Task	Reference/Notes	✔
6.	Install the Avaya Breeze® platform license file, if needed.	Installing the Avaya Breeze platform license file on page 15 Upgrading Avaya Breeze® platform to Release 3.9 does not require a new Avaya Breeze® platform license file. However, if you are upgrading System Manager to higher versions, you must install a new Avaya Breeze® platform license, unless you use SDM client for the System Manager upgrade.	
Complete the following steps on the Avaya Aura® Media Server.			
7.	Verify that Avaya Aura® Media Server is administered for REST.	Administering Avaya Aura Media Server for REST on page 26 Avaya Aura® Media Server must be enrolled on System Manager. For additional information, see the System Manager enrollment section in *Implementing and Administering Avaya Aura® Media Server*.	
8.	Verify Avaya Aura® Media Server is assigned for use with Avaya Breeze® platform.	Assigning Avaya Aura Media Server for use with Avaya Breeze platform on page 28	
9.	Verify SIP and SRTP administration.	SIPS and SRTP on Avaya Aura Media Server on page 28	
10.	Verify digit relay settings.	Enabling and configuring digit relay settings on page 29	
Verify or complete the following steps for certificate management among the components.			
11.	Install the Avaya Aura® System Manager Root CA certificate on each Avaya Breeze® platform node. If you are using a third-party CA, install that CA certificate instead of the System Manager CA.	Installing the Avaya Aura System Manager certificate on Avaya Breeze platform on page 31	
12.	Install the Avaya Breeze® platform System Manager Root CA certificate on Session Manager. If you are using a third-party CA, install that CA certificate instead of the System Manager CA.	Installing the Avaya Breeze platform System Manager certificate on Session Manager on page 32	
13.	Install the Avaya Aura® System Manager Root CA certificate on Avaya Aura® Media Server. If you are using a third-party CA, install that CA certificate instead of the System Manager CA.	Installing the System Manager certificate on Avaya Aura Media Server on page 33	

Chapter 10: Additional information

The following resources provide additional information.

Related links

Documentation on page 43
Training on page 47
Avaya Breeze platform videos on page 48
Viewing Avaya Mentor videos on page 49
Developer resources on page 49
Support on page 50

Documentation

See the following related documents at https://support.avaya.com. Many documents are also available at https://documentation.avaya.com.

Overview

Title	Use this document to:	Audience
Avaya Breeze® platform Overview and Specification	Understand the Avaya Breeze® platform, customer requirements, and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Avaya Aura® System Manager Overview and Specification	Understand System Manager customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel

Table continues…

Title	Use this document to:	Audience
Avaya Aura® Media Server Overview and Specification	Understand Avaya Aura® Media Server customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel

Deploying

Title	Use this document to:	Audience
Deploying Avaya Breeze® platform	Deploy and configure Avaya Breeze® platform. This is the main deployment document for Avaya Breeze® platform. The deployment documents for other environments are listed below.	Implementation engineers Support personnel System administrators
Deploying Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform	Deploy Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform.	Implementation engineers Support personnel System administrators
Quick Start to deploying the HelloWorld Snap-in	Install, configure, and test an Avaya Breeze® platform snap-in service, specifically the HelloWorld call intercept snap-in.	Programmers System administrators
Planning for Deploying Avaya Aura® applications	Understand deployment options for various Avaya Aura® applications.	Services and support personnel System administrators
Deploying and Updating Avaya Aura® Media Server Appliance	Deploy and configure Avaya Aura® Media Server when it is installed on customer-provided servers.	System administrators Services and support personnel
Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment	Deploy and configure Avaya Aura® System Manager in an IaaS environment. A separate document is also available for deploying System Manager in a virtualized environment.	System administrators Services and support personnel

Administering

Title	Use this document to:	Audience
Administering Avaya Breeze® platform	Administer Avaya Breeze® platform and snap-ins.	System Administrators Services and Support personnel

Table continues…

Title	Use this document to:	Audience
Implementing and Administering Avaya Aura® Media Server	Deploy and configure Avaya Aura® Media Server.	System administrators Services and support personnel
Administering Avaya Aura® System Manager	Administer Avaya Aura® System Manager.	System Administrators Services and support personnel
Administering Avaya Aura® Session Manager	Administer Avaya Aura® Session Manager.	System Administrators Services and support personnel
Administering Avaya Session Border Controller	Administer Avaya SBC.	System Administrators Services and support personnel

Maintaining and troubleshooting

Title	Use this document to:	Audience
Upgrading Avaya Breeze® platform	Upgrade Avaya Breeze® platform.	Services and support personnel
Maintaining and Troubleshooting Avaya Breeze® platform	Troubleshoot Avaya Breeze® platform.	Services and support personnel System administrators
Troubleshooting Avaya Aura® System Manager	Troubleshoot System Manager.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Troubleshoot Avaya Aura® Session Manager.	Services and support personnel

Programming

The following developer documents are available on Avaya DevConnect .

Title	Use this document to:	Audience
Getting Started with the Avaya Breeze® platform SDK	Deploy and configure the Eclipse IDE, Apache Maven, and the Avaya Breeze® platform SDK.	Programmers
Avaya Breeze® platform Snap-in Development Guide	Understand the key concepts needed to develop the different types of Avaya Breeze® platform snap-ins.	Programmers
Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers	Troubleshoot Avaya Breeze® platform snap-in developer issues.	Programmers
Avaya Breeze® platform API Javadocs	Understand API classes and uses.	Programmers

Related links

Additional information on page 43
Finding documents on the Avaya Support website on page 46
Avaya Documentation Center navigation on page 46

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Related links

Documentation on page 43

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Related links

Documentation on page 43

Training

The following courses are available on the Avaya Learning website at https://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field, and click **Go** to search for the course.

Course code	Course title
43750W	Selling Avaya Custom and Integration Solutions

Table continues…

Course code	Course title
30210W	Avaya Breeze® platform Overview for Design
30810W	Designing the Avaya Breeze® Solution Part 1 of 2
30820W	Designing the Avaya Breeze® Solution Part 2 of 2
39220W	Avaya Breeze® Release 3.8 Details for Pre-Sales
39240W	Avaya Breeze® UC Snap-ins Release 3.8 Details for Pre-Sales
2016W	Avaya Breeze® platform Fundamentals
20240W	Programming Avaya Breeze® platform Snap-ins Using Java SDK
20250W	Creating Avaya Breeze® platform Workflows Using Engagement Designer
20260W	Creating Advanced Avaya Breeze® platform Workflows Using Engagement Designer
7016W	Avaya Breeze® platform Implementation and Support
71300V	Integrating Avaya Aura® Communication Applications
72300V	Supporting Avaya Aura® Communication Applications

Related links

Additional information on page 43

Avaya Breeze® platform videos

Avaya Breeze® platform provides the following videos to help in the development and deployment of snap-ins. Access these videos at https://www.avaya.com/breezedeveloper.

Title	Audience
Getting Started with the Avaya Breeze® platform SDK: Windows	Programmers
Getting Started with the Avaya Breeze® platform SDK: Linux	Programmers
Creating Your First Service — Part 1	Programmers
Creating Your First Service — Part 2	Programmers
Server Installation and Configuration with vCenter	System Administrators, Services, and Support personnel
Server Installation and Configuration without vCenter	System Administrators, Services, and Support personnel
Service Installation, Configuration, and Test	Programmers
Understanding the Hello Sample Service	Programmers
Understanding the Multi-Channel Broadcast Sample Service	Programmers
Understanding the Whitelist Sample Service	Programmers

Related links

Additional information on page 43

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Related links

Additional information on page 43

Developer resources

Avaya DevConnect provides resources for Avaya Breeze® platform developers.

You must register to access the DevConnect website.

Basic DevConnect membership is free and gives you access to the following information and resources:

- Programming and product documentation
- Sample applications
- Videos

- Webinar recordings
- Forums

Upgraded membership options offer developer-oriented technical support and other program services.

Use a browser to navigate to the Avaya Breeze® platform DevConnect website at https://www.avaya.com/breezedeveloper.

Related links

Additional information on page 43

Support

Platform support

Go to the Avaya Support website at https://support.avaya.com/ for the most up-to-date documentation and product notices. You can also search for release notes, service packs, and patches. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Product documentation is also available on the Avaya Documentation Center at https://documentation.avaya.com.

Developer support

Go to the Avaya DevConnect website at http://www.avaya.com/breezedeveloper to access the Avaya Breeze® platform API, SDK, sample applications, developer-oriented technical documentation, and training materials.

Related links

Additional information on page 43
Using the Avaya InSite Knowledge Base on page 50

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.

   The system displays the Avaya Support page.
5. Click **Support by Product** > **Product-specific Support**.
6. In **Enter Product Name**, enter the product, and press `Enter`.
7. Select the product from the list, and select a release.
8. Click the **Technical Solutions** tab to see articles.
9. Select **Related Information**.

Related links

Support on page 50

Index

A

accepting new service 21
administering
    Avaya Breeze® platform 17
application sequences
    creating 36
assigning
    media server 28
assigning to users
    service profile 39
Avaya Aura Media Server
    adding the System Manager IP address 25
    licensing 14

C

certificate management 31
    Avaya Aura Media Server 33
    Avaya Aura System Manager 31
    Avaya Breeze platform System Manager 32
    legacy System Manager 33
    Session Manager 32
checklist
    configuration 11
    upgrade 41
cluster
    accepting new service 21
clusters
    create 18
    new 18
    view 18
    view attributes 18
collection
    delete 46
    edit name 46
    generating PDF 46
    sharing content 46
content
    publishing PDF output 46
    searching 46
    sharing 46
    sort by last updated 46
    watching for updates 46
creating
    application 36
    application sequence 36
creating a new cluster 18
creating a virtual SIP entity
    session manager 16

D

DevConnect 49
document changes 8
documentation center 46
    finding content 46
    navigation 46
documentation portal 46
    finding content 46
    navigation 46

E

Engagement Call Control 9
entity link
    verification 34

F

finding content on documentation center 46

I

implicit users applications for SIP users 24
InSite Knowledge Base 50

L

license file install
    Avaya Aura Media Server 15
    Avaya Breeze® platform 15
licensing
    Avaya Aura Media Server 14
    file install 14

M

management link verification 22
My Docs 46

P

prerequisites 7

R

replication status verification 35
REST 26
routing calls
    example 36

S

searching for content 46
service profile
adding services 38
assigning to users 39
creating 38
selecting a service version 38
services
adding to a service profile 38
selecting a version for a service profile 38
sharing content 46
SIP entity
Avaya Breeze® platform 16
Collaboration Environment 23
SIPS 28
sort documents by last updated 46
SRTP 28
support 50
System Manager compatibility 9
System Manager IP address for AAMS 25

T

TLS 21
training 47

U

upgradeSolution script
System Manager 9

V

verification
entity link 34
management link 22
replication status 35
videos 49
viewing cluster attributes 18

W

watch list 46